# Pergunta 3

## Experiência 3.1

Nesta alínea o objetivo seria correr o programa ssh-audit para analisar o servidor r *algo.paranoidjasmine.com* O resultado dessa execução foi o seguinte:

```
# general
(gen) banner: SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u5
(gen) software: OpenSSH 7.4p1
(gen) compatibility: OpenSSH 7.3+, Dropbear SSH 2016.73+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256               -- [warn] unknown algorithm
(kex) curve25519-sha256@libssh.org    -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(kex) diffie-hellman-group16-sha512   -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(kex) diffie-hellman-group18-sha512   -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group14-sha256   -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73

# host-key algorithms
(key) ssh-rsa                         -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
(key) rsa-sha2-512                    -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256                    -- [info] available since OpenSSH 7.2

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com   -- [info] available since OpenSSH 6.5
                                      `- [info] default cipher since OpenSSH 6.9.
(enc) aes128-ctr                      -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr                      -- [info] available since OpenSSH 3.7
(enc) aes256-ctr                      -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes128-gcm@openssh.com          -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com          -- [info] available since OpenSSH 6.2

# message authentication code algorithms
(mac) umac-128-etm@openssh.com        -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com   -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com   -- [info] available since OpenSSH 6.2

# algorithm recommendations (for OpenSSH 7.4)
(rec) +ssh-ed25519                    -- key algorithm to append
```

Como podemos observar pela imagem com esta auditoria foi possível retirar bastante informação do servidor, até mesmo o sistema operativo utilizado e a sua versão. Verificamos então que este servidor utiliza o SSH na versão 7.4p1 e neste momento está a correr num Debian versão 10. Em relação aos algoritmos utilizados, tudo parece estar em conformidade, à exceção do algoritmo de troca de chave *curve25519-sha256* que não é reconhecido pela ferramenta.

## Pergunta 3.1

Para responder a esta Pergunta as empresas cotadas no PSI20 escolhidas foram: *Vodafone Portugal e MEO.*

### MEO

O servidor escolhido da MEO foi o seguinte: 62.48.207.171 e os resultados obtidos são:

```
# general
(gen) banner: SSH-2.0-dropbear_2016.74
(gen) software: Dropbear SSH 2016.74
(gen) compatibility: OpenSSH 3.9-6.6, Dropbear SSH 2013.57+
(gen) compression: disabled

# key exchange algorithms
(kex) diffie-hellman-group14-sha1  -- [warn] using weak hashing algorithm
                                   `- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
(kex) diffie-hellman-group1-sha1   -- [fail] removed (in server) since OpenSSH 6.7, unsafe alg
orithm
                                   `- [fail] disabled (in client) since OpenSSH 7.0, logjam at
tack
                                   `- [warn] using small 1024-bit modulus
                                   `- [warn] using weak hashing algorithm
                                   `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
(kex) kexguess2@matt.ucc.asn.au    -- [info] available since Dropbear SSH 2013.57

# host-key algorithms
(key) ssh-rsa                      -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28


# encryption algorithms (ciphers)
(enc) aes128-ctr                   -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes256-ctr                   -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52

# message authentication code algorithms
(mac) hmac-sha1                    -- [warn] using encrypt-and-MAC mode
                                   `- [warn] using weak hashing algorithm
                                   `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-md5                     -- [fail] removed (in server) since OpenSSH 6.7, unsafe alg
orithm
                                   `- [warn] disabled (in client) since OpenSSH 7.2, legacy al
gorithm
                                   `- [warn] using encrypt-and-MAC mode
                                   `- [warn] using weak hashing algorithm
                                   `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# algorithm recommendations (for Dropbear SSH 2016.74)
(rec) -diffie-hellman-group1-sha1  -- kex algorithm to remove
(rec) -diffie-hellman-group14-sha1 -- kex algorithm to remove
(rec) +diffie-hellman-group14-sha256-- kex algorithm to append
(rec) +curve25519-sha256@libssh.org-- kex algorithm to append
(rec) +diffie-hellman-group16-sha512-- kex algorithm to append
(rec) +3des-ctr                    -- enc algorithm to append
(rec) +twofish128-ctr              -- enc algorithm to append
(rec) +twofish256-ctr              -- enc algorithm to append
(rec) -hmac-md5                    -- mac algorithm to remove
```

Pela imagem percebemos que a versão do ssh é a *SSH 2016.74*. Em relação aos algoritmos utilizados, existem alguns *warnings* por se estarem a utilizar algoritmos que já são considerados fracos hoje em dia. A vulnerabilidades encontradas para esta versão do SSH foram as seguintes: CVE-2017-9079 e CVE-2017-9078.

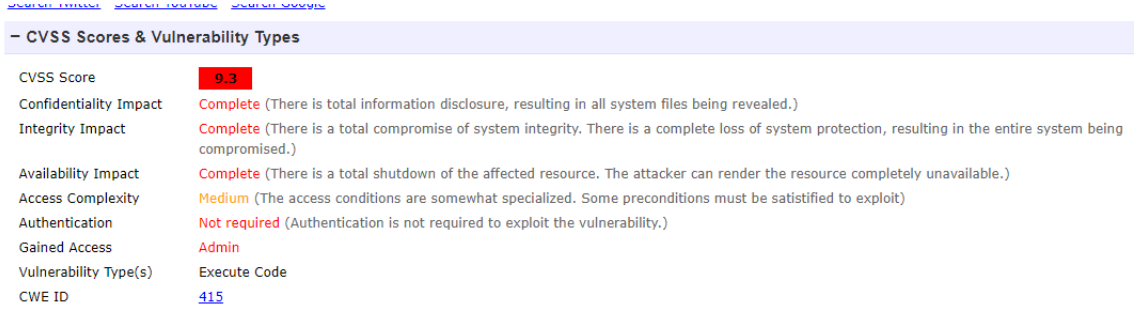
*CVE-2017-9079*

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | **4.7** |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | |
| CWE ID | 264 |

Esta vulnerabilidade permite que utilizadores locais consigam ler alguns ficheiros como se fossem *root*. Para isso o ficheiro tem o *authorized_keys com o comando options.* Esta vulnerabilidade é de gravidade mediana.

*CVE-2017-9078.*



**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | Admin |
| Vulnerability Type(s) | Execute Code |
| CWE ID | 415 |

Esta vulnerabilidade pode levar a execução arbitrária de código como *root* e consequentemente ao comprometimento total do servidor. É de gravidade extrema.

## Vodafone Portugal

O servidor escolhido da Vodafone foi o seguinte: 5.249.25.44 e os resultados obtidos são:

```
root@CSI:~/Tools/ssh-audit# more VodafoneResposta.txt
# general
(gen) banner: SSH-2.0-OpenSSH_7.9
(gen) software: OpenSSH 7.9
(gen) compatibility: OpenSSH 7.2+, Dropbear SSH 2013.62+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.5, Dropbear SS
H 2013.62
(kex) diffie-hellman-group-exchange-sha256  -- [warn] using custom size modulus (possibly weak
)
                                            `- [info] available since OpenSSH 4.4

# host-key algorithms
(key) rsa-sha2-512                          -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256                          -- [info] available since OpenSSH 7.2
(key) ssh-rsa                               -- [info] available since OpenSSH 2.5.0, Dropbear
SSH 0.28
(key) ssh-ed25519                           -- [info] available since OpenSSH 6.5

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com         -- [info] available since OpenSSH 6.5
                                            `- [info] default cipher since OpenSSH 6.9.
(enc) aes256-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes128-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes256-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SS
H 0.52
(enc) aes192-ctr                            -- [info] available since OpenSSH 3.7
(enc) aes128-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SS
H 0.52

# message authentication code algorithms
(mac) umac-64-etm@openssh.com               -- [warn] using small 64-bit tag size
                                            `- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com              -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com             -- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 6.2
(mac) umac-64@openssh.com                   -- [warn] using encrypt-and-MAC mode
                                            `- [warn] using small 64-bit tag size
                                            `- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com                  -- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256                         -- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9, Dropbear SSH 2013
.56
(mac) hmac-sha2-512                         -- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9, Dropbear SSH 2013
.56
(mac) hmac-sha1                             -- [warn] using encrypt-and-MAC mode
                                            `- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
```

```
# algorithm recommendations (for OpenSSH 7.9)
(rec) -diffie-hellman-group-exchange-sha256 -- kex algorithm to remove
(rec) +diffie-hellman-group18-sha512        -- kex algorithm to append
(rec) +diffie-hellman-group14-sha256        -- kex algorithm to append
(rec) +diffie-hellman-group16-sha512        -- kex algorithm to append
(rec) -hmac-sha2-512                        -- mac algorithm to remove
(rec) -umac-128@openssh.com                 -- mac algorithm to remove
(rec) -hmac-sha2-256                        -- mac algorithm to remove
(rec) -umac-64@openssh.com                  -- mac algorithm to remove
(rec) -hmac-sha1                            -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com            -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com              -- mac algorithm to remove
```

Pelos resultados do ssh-audit é possível perceber que a versão do ssh utilizada é a *OpenSSH 7.9.* Em relação aos algoritmos suportados são também apresentados alguns avisos pela utilização de alguns parâmetros com poucos bits (exemplo: tag-size com 64 bits), modos de autenticação cifrada pouco seguros como o *encrypt-and-mac* e até mesmo algoritmos de hash considerados fracos como o sha-1. Em relação as vulnerabilidades, apesar das versões anteriores possuírem várias vulnerabilidades publicamente conhecidas, nesta versão encontramos apenas a CVE-2018-20685.

### *CVE-2018-20685*

Esta vulnerabilidade permite ultrapassar restrições de acesso através da manipulação do nome de ficheiros (deixando-o vazio ou com um “.”). No entanto, esta falha não está devidamente documentada, como é possível observar pela imagem.

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 0.0 |
| Confidentiality Impact | ??? |
| Integrity Impact | ??? |
| Availability Impact | ??? |
| Access Complexity | ??? |
| Authentication | ??? |
| Gained Access | None |
| Vulnerability Type(s) | Bypass a restriction or similar |
| CWE ID | CWE id is not defined for this vulnerability |

## Conclusão

Após análise dos resultados obtidos com os diferentes servidores podemos concluir então, que neste caso, nenhum apresentava um grande número de vulnerabilidades (3 no total). A vulnerabilidade mais grave está indiscutivelmente presente no primeiro servidor (MEO), visto ter um CVSS score de 9.3 em 10, significando que os 3 pilares da segurança (Disponibilidade, Integridade, Confidencialidade) eram completamente quebrados.